دور المراجعة العامة المتبادلة باستخدام تقنية سلاسل الثقة في مراجعة بيانات المصادر الخارجية للتخزين السحابى

رانيا رضا محفوظ[1]

ملخص البحث :

تناول هذا البحث أنه مع النمو السريع للبيانات ، والمحدودة بسعة التخزين ، يختار كثير من تطبيقات إنترنت الأشياء الاستعانة بالمصادر الخارجية للبيانات لمقدمى الخدمة السحابية ، ولكن في مثل تلك الحالات يمكن أن تتلف البيانات المستعان بها في التخزين السحابي بسهولة ويصعب العثور عليها في الوقت المناسب ، مما يؤدي إلى حدوث مشكلات أمنية محتملة, لذلك فقد تم بحث بروتوكول حيازة البيانات القابلة للإثبات على نطاق واسع نظرا لقدرته على تدعيم المراجعة الفعالة للبيانات ذات المصادر الخارجية في السحابة ومع ذلك ، تتطلب معظم مخططات حيازة البيانات القابلة للإثبات مراجع الطرف الثالث لمراجعة البيانات لمالكي البيانات ، الأمر الذي يتطلب أن يكون مراجع الطرف الثالث جديرًا بالثقة وعادلاً. وهذا ما قد لا يحدث في الواقع ولتحديد الإستعانة بمراجع الطرف الثالث ، نتناول المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة لبيانات المصادر الخارجية للتخزين السحابى.وذلك من خلال بنية سلسلة مراجعة تستند إلى آلية التحفيز التي تعتمد على الائتمان للسماح لمقدمي الخدمات السحابية بمراجعة بعضهم البعض بشكل متبادل مع منع التواطؤ.

الكلمات الرئيسية :

تقنية سلاسل الثقة – التخزين السحابى – المراجعة العامة المتبادلة – الخدمات السحابية .

Abstract:

This research addressed that with the rapid growth of data, and limited storage capacity, many IoT applications choose to outsource data to cloud service providers, but in such cases the data outsourced in cloud storage can be easily corrupted and difficult to find in time, which This leads to potential security issues, so the provable data acquisition protocol has been extensively researched due to its ability to underpin effective auditing of outsourced data in the cloud. which requires the third-party auditor to be trustworthy and fair. This may not happen in reality and to determine the use of third-party auditors, we address public mutual auditing using the Blockchain technology of data from external sources of cloud storage. This is through a review chain structure based on the credit-based incentive mechanism to allow the cloud service providers to review each other mutually with collusion prevention

Keywords:

Blockchain technology - cloud storage - public mutual auditing - cloud services.

[1] مدرس مساعد بقسم المحاسبة والمراجعة – كلية التجارة – جامعة السويس

أولا: الإطار العام للبحث :

١. المقدمة وطبيعة المشكلة :

مع التقدم التكنولوجي السريع في إنترنت الأشياء (IoT) . زادت المحطات (النهايات الطرفية) وزاد كفاءة نقل المعلومات مما يعني أيضًا زيادة كمية البيانات مع توفير المزيد من الملاءمة ، ضخامة بيانات النهايات الطرفية وسعة التخزين المحدودة جعلت تطبيقات إنترنت الأشياء يجب أن تتحول إلى مقدمى الخدمات السحابية (CSPs) للحصول على دعم سعة تخزين البيانات الاحترافي كمالكي البيانات (DOs). وبمعنى آخر، تعزز التطورات التكنولوجية تكامل الخدمات السحابية وإنترنت الأشياء. ومع ذلك ، لا توفر الخدمات السحابية الملاءمة لإنترنت الأشياء فحسب ، بل تتحدى أيضًا خصوصية وأمن البيانات الناتجة عن النهايات الطرفية ، نظرًا لأنه يتم تخزين البيانات في السحابة ، سيفقد مالك البيانات السيطرة القوية على البيانات. قد يتعرض مقدمى الخدمات السحابية للفساد بسبب التهديدات الخارجية ، مثل القرصنة أو الكوارث الطبيعية ، وحتى أنهم قد يتلاعبون بالبيانات لمصلحتهم الخاصة. هذه التهديدات الخارجية والداخلية يمكن أن تضر بسلامة البيانات البعيدة . (X. Jia, 2018, p. 1)

في حالة عدم القدرة على مراجعة سلامة البيانات في الوقت المناسب ، مع وجود تلف فى البيانات المستخدمة في الحساب أو التشغيل الرئيسي ، ذلك سوف يؤدى إلى حدوث كوارث لا حصر لها. يمكن لتكنولوجيا المراجعة عن بعد لبيانات المصادر الخارجية ضمان تكامل البيانات بنسبة قليلة من التفاعل ، والتي يمكنها فقط حل مشاكل الأمان. حيث أن مشكلة الثقة متعددة الأطراف في مراجعة سلامة البيانات التقليدية تزيد من ضرورة الاتجاه الحتمي لدمج تقنية blockchain في مراجعة سلامة البيانات ،على الرغم أن تقنية blockchain الشائعة ممكن أن تتجنب مشكلة التواطؤ بسبب مجالها الكبير من نقط التوافق وآلية التحفيز الفعال إلا أنه من الصعب الوصول إلى أداء مقبول وكفء في ظل وجود مراجعة واسعة النطاق. (Hanzhe Yang, June 2021, p. 1)

لذلك تعتمد المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة PMAB على Consortium Blockchain ، حيث يتم ضمان الإشراف المتبادل من خلال فعالية آلية التحفيز القائمة على الائتمان ، والتي تعزز الإشراف على مقدمي الخدمات السحابية أثناء مراجعة البيانات ، ونظرًا لعدم وجود تصميم blockchain مخصص لبروتوكول المراجعة ، لا تزال المخططات الحالية تعاني من التكلفة الزائدة والتعرض للتواطؤ والاحتيال. لذلك تحاول الدارسة تغطية هذه الفجوة البحثية عن طريق تناول المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة لبيانات المصادر الخارجية للتخزين السحابى لحل مشاكل الاحتيال والتواطؤ في المخطط العام للمراجعة ،وتقليل تكلفة المراجعة بشكل كبير وتحسين كفاءة المراجعة .

٢. أهمية البحث :

يحقق البحث أهمية خاصة في المجالين الأكاديمي والعملي :

- **الأهمية الأكاديمية : تناول البحث موضوع بحثي مثار اهتمام أدبيات الفكر المحاسبي في ظل التوجه العالمي نحو تبنى المراجعة العامة المتبادلة لبيانات المصادر الخارجية للتخزين السحابى، فهناك ندرة نسبية في الدارسات التي تناولت دور المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة في مراجعة بيانات المصادر الخارجية للتخزين السحابى ، لذلك يكتسب البحث أهمية بمحاولته تحليل طبيعة التخزين**

السحابى وبيان لأهمية تطوير تقنيات مراجعة بيانات المصادر الخارجية للتخزين السحابى من خلال المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة .

- الأهمية العملية : تنبع الأهمية العملية للبحث حيث تفتقر خدمات التخزين السحابية إلى الشفافية واللامركزية المحدودة بالإضافة إلى التحديات المتعلقة بالخصوصية مما يؤثر على سرية البيانات المخزنة وسلامتها وتوافرها ولذلك كان هناك ضرورة لتطوير تقنيات المراجعة لمواجهة تلك التحديات .

٣. هدف البحث : تسعى الدراسة لتحقيق هدف رئيسي متمثل في تحليل طبيعة التخزين السحابى وتقنية سلاسل الثقة وبيان دور المراجعة العامة المتبادلة بالتكامل مع تقنية سلاسل الثقة في مراجعة بيانات المصادر الخارجية للتخزين السحابى .

٤. فروض ومتغيرات البحث :

- الفرض الرئيسي: (لا يؤدى استخدام المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة إلى تفعيل مراجعة بيانات المصادر الخارجية للتخزين السحابى) .
- متغيرات البحث: المتغير المستقل (X1) المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة، المتغير التابع (Y2) مراجعة بيانات المصادر الخارجية للتخزين السحابى .

٥. منهج البحث : في ضوء مشكلة وأهمية وهدف البحث، سيتم اتباع المنهجين الاستقرائي والاستنباطي وذلك على النحو التالي :

- المنهج الاستقرائي: أتبعت الباحثة المنهج الاستقرائي فقامت بدراسة وتحليل عدداً من الدراسات والبحوث والمراجع العلمية التي تناولت موضوع البحث أو أحد جوانبه، وكذلك المؤتمرات العلمية، والدراسات والتشريعات المحلية والدولية التي قامت بها المنظمات الداعمة للمراجعة العامة المتبادلة ، وذلك سعياً منها لفهمها وتحليلها للتوصل إلى النقاط التى يمكن الاستناد عليها في موضوع البحث .
- المنهج الاستنباطي: استخدمت الباحثة هذا المنهج بغرض الكشف عن النتائج المنطقية المترتبة على اختبار فرض الدراسة الأساسي وذلك من خلال التحليل النظري .

٦. حدود البحث : تقتصر حدود البحث على دراسة وتحليل مجموعة محددة من نماذج تقنية سلاسل الثقة Ouroboros Blockchain بما يحقق هدف البحث .

٧. تقسيمات البحث : ومن أجل تحقيق الأهداف السابقة قامت الباحثة بتقسيم البحث إلى العناصر الرئيسية التالية:

أولا: تحليل طبيعة التخزين السحابى .

ثانياً : تحليل طبيعة تقنية سلاسل الثقة Blockchain.

ثالثا: المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة لبيانات المصادر الخارجية للتخزين السحابى.

أولا: تحليل طبيعة التخزين السحابى :

١. مفهوم التخزين السحابى :

يعد التخزين السحابي من أبرز الخدمات التي تقدمها شركات الإنترنت في الفترة الحالية، وهو الشيء الذي لم يكن بالإمكان تخيله واقعا؛ نظرا لكثير من العوائق التقنية والمادية المختلفة، وأصبح الآن بمقدور كل شخص أن يمتلك قدرة الوصول، والتعامل والتحكم بملفاته الرقمية الخاصة والمهمة في أي وقت، ومن أي مكان عبر المنصات

المختلفة، خلال الاتصال بالشبكة العالمية والاشتراك في خدمات التخزين السحابي. يعد التخزين السحابي ثورة حفظ البيانات والمعلومات على الانترنت، وهو بمثابة البنية التحتية للحوسبة السحابية. وهو واحد من العديد من الخدمات التي تقدمها الحوسبة السحابية لذلك فهو خدمة من خلالها يمكن للمستخدم الاستعانة بمصادر خارجية لتخزين البيانات الخاصة به. (محمود م.، ٢٠١٥، صفحة ٢٤) .

٢. كيفية الاستفادة من خدمات التخزين السحابي:

للاستفادة من تلك الخدمات يتطلب الأمر فقط التسجيل فيها للحصول على مساحة مجانية للتخزين ومشاركة الملفات من خلالها والقيام بمهام أخرى، وفي حالة الحصول على مساحة أكبر، فإن تلك الخدمات تقبل ذلك بشرط الدفع شهريا أو سنويا؛ للحصول على المساحة المطلوبة. (محمود م.، ٢٠١٦، صفحة ٢٠٦)

وفرت الخدمة السحابية الوصول إلى الخوادم وقواعد البيانات والتخزين وأي خدمات تطبيقات عبر الإنترنت. سيؤدي ذلك إلى تسهيل وصول المستخدم إلى البيانات في كل مكان فقط باستخدام اتصال الإنترنت من أي جهاز. تتيح الخدمة السحابية للمستخدمين تشغيل التطبيق للعديد من مستخدمي الأجهزة المحمولة أو لدعم العمليات التجارية الهامة. حيث توفر الخدمة السحابية الوصول السريع إلى موارد تكنولوجيا المعلومات المرنة ومنخفضة التكلفة. باستخدام تقنية الخدمة السحابية . (M Husni, 2020, p. 1)

٣. تحليل طبيعة مقدمى الخدمات السحابية (CSP) :

مقدم الخدمة السحابية" أو CSP هي مؤسسة تستضيف جميع الخدمات مثل الشبكات والبرامج والخوادم والبنية التحتية والمزيد. بالإضافة إلى ذلك ، يقومون أيضًا بتوظيف الموظفين وإدارتهم ، وتوفير الأمن للخدمات التي يقدمونها. هذا يعفي المنظمات العميلة من مسؤوليتها الفردية في إعداد بنيتها التحتية وإدارتها. بعض الأمثلة الشائعة لمقدمى الخدمات السحابية هي "Amazon Web services" وMicrosoft Azure و Salesforce و Google Cloud platform وغيرهم. (Manikandan, Dec 30, 2019)

٤. واجبات مقدمى خدمة التخزين السحابي:

من واجبات مقدمى خدمة التخزين السحابي : (محمود م.، ٢٠١٥) (Nath, Nishant, Feb 17,2021)

- **حماية البيانات data protection حيث يجب أن يتم التخزين بشكل آمن، وأن تكون البيانات قادرة على التحرك بشكل آمن من موقع إلى آخر, ومشفرة وفق أفضل تقنيات التشفير.**
- **يجب الفصل الصحيح والكامل بين الواجبات والوظائف (segregation of duties) حتى يضمن أن خدمات كالمراقبة والرصد والمراجعة يجب الفصل بينهم، وتطبيق نظام متكامل لضمان عدم تسرب البيانات.**
- **توفير إدارة الهوية والتحكم بالدخول للمصادر المعلوماتية وموارد الخدمة وفقا لاحتياجات المستخدم .**
- **مقدم الخدمة لابد أن يضمن السرية التامة للبيانات بكل أنواعها, وعدم السماح بالوصول لها إلا للأشخاص المخولين من قبل المستخدم .**

- **دور مقدمى الخدمات السحابية لا يقتصر على تحسين العمليات التجارية ويعزز كفاءة البنية التحتية لتكنولوجيا المعلومات فحسب ، بل يقلل أيضًا من تكاليف تشغيل مرافق تكنولوجيا المعلومات في الموقع وترقيتها وصيانتها.**
- **يتأكد من الحصول على بيانات عالية الجودة لتحليلها بدقة.**
- **ينشر مقدمى الخدمات السحابية أدوات معقدة لتنظيم البيانات لإخراج معلومات مفيدة لاستخدامها في قرارات الأعمال الحاسمة.**

وبالرغم من ذلك يواجه التخزين السحابي أيضًا العديد من التهديدات الأمنية الداخلية والخارجية يمكن تلخيصها في النقاط التالية : (Danilo Francati, May 2021) (Hongtao Li, 2021)

- **قد يبذل المخترقون قصارى جهدهم لاسترداد بيانات المستخدمين الخارجية ، لتدمير وحذف البيانات الخارجية. بعد ذلك ، يتم إتلاف سرية وسلامة وتوافر بيانات المستخدمين المخزنة.**
- **قد يتم أيضًا التلاعب ببيانات المستخدم الخارجية بشكل غير قانوني بواسطة مقدم الخدمة السحابية CSP. علاوة على ذلك ، قد يقوم مقدم الخدمة السحابية CSP بحذف البيانات التي نادرًا ما يصل إليها المستخدمون العاديون من أجل تقليل مساحة التخزين وتوفير النطاق الترددي .**
- **قد لا يتمكن المستخدمون من معرفة التغييرات في البيانات في الوقت المناسب وقد يفتقرون إلى الثقة في مقدم الخدمة السحابية CSP ثم تنشأ الخلافات ، على الرغم من أن هذه الخلافات قد تكون ناجمة عن عمليات المستخدمين غير الصحيحة.**

وبذلك تفتقر خدمات التخزين السحابية إلى الشفافية واللامركزية المحدودة بالإضافة إلى التحديات المتعلقة بالخصوصية والأمان. ومع استمرار تزايد الحاجة إلى حلول بيانات أكثر مرونة وخصوصية وأمانًا بشكل كبير ، فإن إعادة التفكير في الهيكل الحالي للتخزين السحابي يعد أمرًا بالغ الأهمية بالنسبة للمؤسسات. لذلك من الأهمية تطوير تقنيات مراجعة البيانات لتصبح فعالة للتحقق من سرية البيانات المخزنة وسلامتها وتوافرها. لذلك يمكن للمستخدمين استخدام تقنية المراجعة عن بُعد للتحقق من صحة البيانات الخارجية. ويتمثل التحدي الأساسي الذي يواجهه مراجعة البيانات السحابية في كيفية القيام بذلك بكفاءة .

لذلك سوف نتناول المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة (Blockchain) لبيانات المصادر الخارجية للتخزين السحابى من خلال الاستفادة من السمات الفريدة لـ blockchain . ويمكن التعرف على طبيعة تقنية سلاسل الثقة (Blockchain) من خلال النقطة التالية .

ثانياً : تحليل طبيعة تقنية سلاسل الثقة Blockchain

١. مفهوم تقنية سلاسل الثقة Blockchain :

يمكن تعريف Blockchain أو تقنية سلاسل الثقة باختصار بأنها قاعدة بيانات عملاقة لا مركزية تحتوي على تشكيلة واسعة من السجلات يتم إنشائها من قبل الأطراف التي تتعامل بها وفق قواعد تحقق جودة عالية ، فهي لا مركزية لكونها لا تخضع لأي سلطة، تتمتع بدرجة أمان عالية، كما أن البيانات التي تضمها سرية ولا يمكن لغير المشاركين على الشبكة الاطلاع عليها، وتتمتع بسرعة عالية، وأخيراً انخفاض تكلفة نقل البيانات أو القيم بين المتعاملين باستخدام تقنية التشفير (Coyne, J.G., & McMickle, P.L, 2017)

وتقنية Blockchain عبارة عن دفتر أستاذ رقمي موزع للمعاملات الموقعة بشكل مشفر والتي يتم تجميعها في شكل كتل. وكل كتلة مرتبطة بشكل مشفر بالكتلة السابقة (لذا يصعب العبث بها بعد التحقق من صحة كل معاملة والتصديق عليه بإجماع الآراء). وعند إضافة كتل جديدة تصبح الكتل القديمة أكثر صعوبة في التعديل (مقاومة للعبث). ويتم نسخ الكتل الجديدة عبر نسخ من دفتر الأستاذ داخل الشبكة، ويتم حل أي تعارض تلقائيا باستخدام سياسات مبرمجة ذاتية. (Dylan Yaga , Peter Mell ,Nik Roby ,Karen Scarfone, 2018, p. 1)

ونظرًا لأن التقنيات الرقمية الجديدة الأخرى (الروبوتات ، والبيانات الضخمة ، والتحليلات ، والذكاء الاصطناعي ، وما إلى ذلك) تحدث ثورة ليس فقط في الطريقة التي تدير بها الشركات أعمالها ولكن أيضًا في طريقة معالجة المعلومات والتواصل بين مختلف أصحاب المصلحة .تعتبر تقنية سلاسل الثقة Blockchain ، التي كانت أصل العملات المشفرة (بشكل أساسي Bitcoin) ، اليوم واحدة من أقوى التقنيات بعد الإنترنت (Najoua Elommal, 2021, p. 2)

٢. مكونات تقنية سلاسل الثقة Blockchain :

تتكون تقنية سلاسل الثقة Blockchain من الآتي: (سيد، ٢٠١٩، صفحة ١٧٩)

- **الكتلة Block: تمثل وحدة بناء Blockchain وهي عبارة عن مجموعة من العمليات أو المعاملات أو المهام المطلوب تنفيذها، وتتكون كل كتلة من رأس الكتلةBlock Header (يشمل بيانات التعريف الخاصة بهذه الكتلة، بيانات الكتلة، رأس الكتلة السابقة، بصمة الكتلة، القيم المناسبة للبحث عن التوقيع الرقمي).**
- **المعاملات Transactions: تمثل المعلومات أو العمليات أو المهام الفرعية داخل الكتلة.**
- **التشفير (الهاش) (Cryptographic Hash): تمثل وظائف تجزئة التشفير Cryptographic Hash Functions الحمض النووي المميز في Blockchain وتستخدم للقيام بالعديد من المهام من أهمها: اشتقاق العنوان المميز لل Blockchain مما يساعد على التمييز بين سلاسل الكتل المختلفة؛ إنشاء تعاريف للمعلومات داخل الكتلة فريدة من نوعها؛ تأمين بيانات الكتلة ؛ تأمين رأس الكتلة.**
- **المفتاح المشفر غير المتماثل Asymmetric-Key Cryptography: تعتمد تقنية Blockchain على نظام تشفير باستخدام زوج من المفاتيح غير المتماثلة – مفتاح عام ومفتاح خاص- ترتبط رياضيا مع بعضها البعض ويمكن تلخيص استخدامهما فيما يلي: تستخدم المفاتيح الخاصة لتوقيع المعاملات رقميا؛ تستخدم المفاتيح العامة لاشتقاق العناوين؛ تقوم المفاتيح العامة بالتحقق من التوقيعات التي تم إنشاؤها باستخدام مفاتيح خاصة؛ يوفر المفتاح غير المتماثل القدرة على التحقق من نقل المستخدم القيمة المستخدم آخر في حوزته المفتاح الخاص والقادر على توقيع العملية التجارية.**
- **العناوين واشتقاق العنوان Addresses and Address Derivation: تستخدم Blockchain عنواناً وهو عبارة عن سلسلة حروف أبجدية و/أو رقمية مستمدة من المفتاح العام المستخدم شبكة Blockchain وباستخدام تجزئة التشفير.**
- **دفاتر Ledgers: دفتر الأستاذ يحتوي على سجلات تاريخية كاملة موثوق فيها أمنه تتسم بالشفافية وتكون متاحة لجميع المشاركين في Blockchain من خلال نسخ متطابقة باستخدام شبكة مباشرة دون الحاجة إلى وسيط مركزي كالبنوك مثلا لضمان هذه المعاملات أو التحقق منها.**

- **الكتل المسلسلة Chaining Blocks: يتم ربط الكتل معا عن طريق Hash فيشكل ذلك سلسلة الكتل Blockchain.**

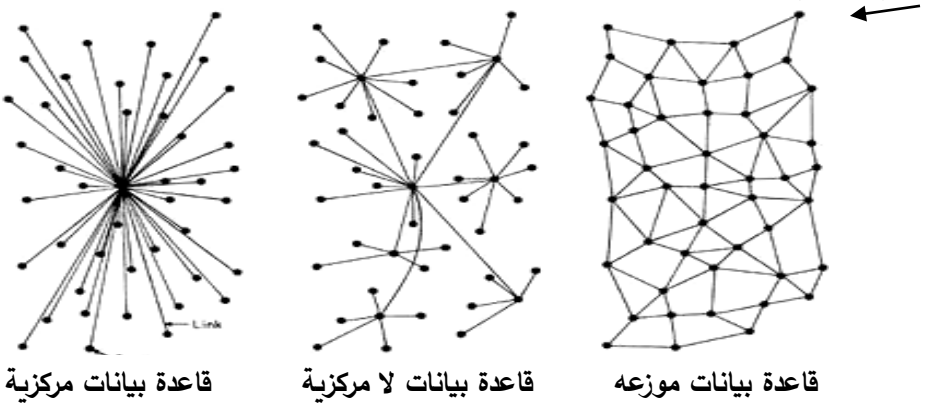
٣. أنواع تقنية سلاسل الثقة Blockchain :

تنقسم تقنية سلاسل الثقة Blockchain إلى سلسلة كتل عامة وسلسلة كتل خاصة وتنقسم كل منهم من حيث من يمكنه قراءة البيانات على الشبكة الى مفتوحة ومغلقة كما يلي : (غازى، ٢٠٢٠، صفحة ٧)

- **سلسلة كتل عامة : يمكن لأي شخص الإنضمام إلى شبكة block chain ، مما يعني أنه يمكنهم قراءة أو كتابة أو مشاركة البيانات والمعلومات مع أعضاء سلسلة كتل ، وتعتبر سلاسل الكتل العامة غير مركزية ، ولا يمكن لأي شخص التحكم في الشبكة وهي آمنة بحيث لا يمكن تغيير البيانات بمجرد التحقق من صحتها في سلسلة الكتل، وتنقسم إلى من حيث من يمكنه قراءة البيانات ومشاركتهم على الشبكة :**
  - **عامة مفتوحة: مثل (العملات – الرهانات–العاب الفيديو).**
  - **عامة مغلقة: مثل (التصويت – سجلات التصويت – المبلغين whistleblower).**
- **سلسلة كتل خاصة: تفرض الشبكات المسموح بها قيودا على من يمكن يسمح له بالمشاركة في الشبكة وفى أي معاملات وتنقسم الى :**
  - **خاصة مفتوحة مثل (سلاسل التوريد– قوائم أرباح الشركة–السجلات المالية الحكومية).**
  - **خاصة مغلقة مثل (العوائد الضريبية–القوات المسلحة– تطبيق القانون law enforcement – الدفاع الوطني –الانشاءات construction).**

٤. آلية تقنية سلاسل الثقة Blockchain : (نخال، ٢٠٢٠، صفحة ٩)

تعتبر Blockchain نوعا خاصا من قواعد البيانات حيث تتميز بعدم مركزية تخزين البيانات، حيث يكون التخزين فيها توزيعيا في نقاط كثيرة منتشرة على الشبكة تسمى العقدNodes وهي عبارة عن أجهزة حاسبات بقدرات عالية من حيث التخزين والمعالجة، أما الأنظمة الحالية فتخزن بياناتها على أجهزة مركزية تعرف بـ Servers والشكل التالي يوضح الفرق بين قاعدة البيانات المركزية والموزعة واللامركزية



وكما يتضح من الشكل السابق تمثل العقد Nodes في قاعدة البيانات الموزعة أجهزة حاسب ذات قدرات عالية تكون مهمتها الرئيسية القيام بوظيفة التحقق من صحة وأصالة (Authenticity) العمليات التي تتم في هذه

الشبكة وذلك ليتم تنفيذها بناء على قواعد آلية التنفيذ على الشبكة وذلك مقابل مكافأة ما يحددها النظام، وتقوم هذه النقاط بتشفير كل عملية وربطها مع العملية السابقة عن طريق تقنية التشفير، كما تمنع من التعديل عليها وترتبط الكتل مع بعضها البعض من خلال ما يعرف بالمفتاح العام (Public key) المستخدم للتعريف بالعملية والمستخدم عبر الشبكة والمفتاح الخاصPrivate key الذي يمتلكه صاحب العملية فقط، وعلمية التشفير هذه تتم عبر تقنية تسمى بمنحنى التشفير وتقوم بالتشفير (Encryption) وفك التشفير(Decryption) لنقل البيانات بطريقة آمنة، وهي التقنية التي تستخدمها اليوم معظم المؤسسات المالية حول العالم في حفظ بياناتها وتأمينها .

٥. خصائص وفوائد تقنية Blockchain :

تحليل blockchain يبرز ثلاث خصائص رئيسية لهذه التكنولوجيا: (Najoua Elommal, 2021, p. 6)

أ. الشفافية وإمكانية التتبع: يحتوي blockchain على معلومات لا يمكن تعديلها أو حذفها ، والتي يشاركها المستخدمون. أيضًا ، يتم تسجيل كل عملية يتم تنفيذها بشكل نهائي في blockchain ، مما يجعل من الممكن تتبع المسار الذي تنتقله كل قطعة من المعلومات المخزنة.

ب. الأمان أو حماية البيانات: يتم تأمين البيانات المسجلة في blockchain عن طريق التشفير ، والمصادقة عليها وغير قابلة للتغيير ، لأن الحظر يزيل الأخطاء ويقلل من مخاطرها.

ج. اللامركزية: تسهل blockchain التعامل بدون الشبكة المركزية ، والتي توفر التحكم والحوكمة في النظام. في الواقع .

د. يسمح blockchain بتسجيل المعاملة كحدث واحد ، مما يوفر الوقت ويقلل بشكل كبير من الأخطاء البشرية والاحتيال.

أشاد العديد من المراجعين لدور blockchain كمصدر "للتحقق" حيث يتم التحقق من صحة المعاملات من خلال العقد في الشبكة ومع ذلك ، غالبًا ما يتم الخلط بين درجة ونوع التحقق الذي يوفره blockchain مقارنة بما يقدمه مراجعى البيانات المالية. كما أنه يوفر فرصة "للتحقق بدون تكلفة" حيث تتم مصادقة المعاملات على blockchain باستخدام آلية إجماع. في الواقع لا تتحقق تقنية سلاسل الثقة blockchain مما إذا كانت المعاملة قد تم حسابها بشكل صحيح بموجب قواعد التقارير المالية أو أن لها غرضًا تجاريًا مشروعًا. بينما تتحقق تقنية سلاسل الثقة blockchain مما إذا كانت المعاملة قد حدثت ومقدارها وفي أي تاريخ ، فإنها لا توفر فحصًا للضوابط الداخلية التي تكمن وراء عملية إعداد التقارير المالية لمنع أو اكتشاف الاحتيال والأخطاء ، كما هو الحال مع مراجعة البيانات المالية. المراجعة هى أكثر بكثير من مجرد التحقق من روتين المعاملات ، كونها تقييمًا شاملاً لجودة الضوابط الداخلية للمؤسسة وسياسات إعداد التقارير المالية ومدى معقولية التقديرات الهامة. هذا النشاط لا يمكن أن يحل محله تقنية سلاسل الثقة . (Erica Pimentel, October 2020, p. 5)

ولذلك نرى أن تقنية سلاسل الثقة blockchain تدعم وظيفة المراجعة لكنها لا تغنى عنها وذلك من خلال تمكين التأكيد المستمر. حيث يستخدم blockchain كمستودع للبيانات بتحديث المعلومات (ومراجعتها) في الوقت الفعلي. (Erica Pimentel, October 2020, p. 7) .

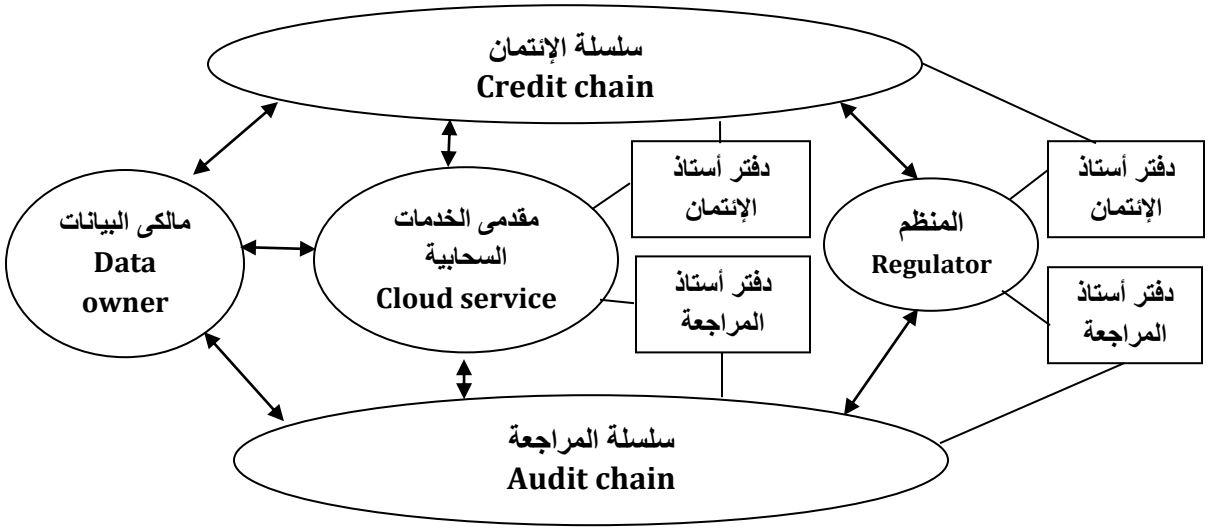
وبالرغم من أهمية المراجعة من قبل طرف ثالث Third public auditor (TPA)، إلا أنه لا يمكن التخلص من احتمال وجود مراجع غير نزيه ، لأنه لا يوجد طرف ثالث موثوق به تمامًا في العالم الحقيقي. على الرغم من أن بعض العلماء قد أجروا أبحاثًا حول مشكلة حماية الخصوصية من قبل مراجع الطرف الثالث Third public auditor (TPA)، بناءً على مخططات المراجعة العامة، إلا إن الطرف الثالث ليس آمنًا بطبيعته. حدثت بعض الحوادث الأمنية بشكل متكرر في السنوات الأخيرة ، مثل تسرب البيانات والعبث بالبيانات. قد يكشف طرف ثالث عن بيانات المستخدم لتفعيل المنفعة الاقتصادية ، من ناحية أخرى ، قد يعلن بعض المستخدمين بشكل ضار عن فقدان البيانات مقابل تعويض مرتفع. بسبب عدم وجود ثقة متبادلة مع مقدمى الخدمات السحابية (CSP) (Song (Chunhua Li, September 2018, p. 335) Li, 2020, p. 1)

وبناءا على ذلك سوف نتناول بنية سلسلة مراجعة تستند إلى آلية التحفيز التي تعتمد على الائتمان للسماح لمقدمي الخدمات السحابية بمراجعة بعضهم البعض بشكل متبادل مع منع التواطؤ .وذلك من خلال النقطة التالية .

ثالثاً : المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة لبيانات المصادر الخارجية للتخزين السحابى :

١. طبيعة المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة : (Hanzhe Yang, June 2021, p. 2)

المراجعة العامة المتبادلة لتقنية سلاسل الثقة (PMAB) يأخذ في الاعتبار سيناريو مراجعة البيانات العامة للبيانات الخارجية في التخزين السحابي ، والذي يتكون بشكل أساسي من مالك البيانات (DO) ومقدمي الخدمات السحابية (CSPs) والمنظم (R) .سلسلة المراجعة وسلسلة الائتمان هما اثنان من دفاتر الأستاذ الموزعة التي يحتفظ بها مقدمي الخدمات السحابية CSPs والمنظم (R) ، والتي على التوالي ، تسجل معلومات المراجعة والائتمان لكل كيان. بعد التحول إلى المصادر الخارجية للبيانات لمقدمي الخدمات السحابية (CSPs) ، ومالك البيانات (DO) يتم عقد المراجعة مع مقدمي الخدمات السحابية (CSPs) والمنظم (R) . ويمكن بيان ذلك من خلال الشكل التالى :



في المراجعة العامة ، يوفر مقدم الخدمات السحابية (CSP) التي تم مراجعتها دليلاً لسلسلة المراجعة ؛ ثم يقوم بعض من مقدمى الخدمات السحابية (CSPs) بالتحقق الكامل من المراجعة وتسوية الائتمان تحت إشراف من

المنظم(R). ويمكن لمالك البيانات (DO) الحصول على نتائج المراجعة والتسوية الائتمانية من خلال دفتري الأستاذ الموزع. ويمكن بيان الأدوار المختلفة لجميع الكيانات في المراجعة العامة المتبادلة لتقنية سلاسل الثقة (PMAB) على النحو التالي:

أ. مالك البيانات (DO) لديه موارد محدودة للاتصال والحساب والتخزين. يحول البيانات إلى مقدمى الخدمات السحابية (CSPs) بعد تحويلها إلى بيانات ذات مصادر خارجية ويحقق المراجعة العامة مع (PMAB) .

ب. يوفر مقدمى الخدمات السحابية (CSPs) لمنصات مالكى البيانات DOs مساحة تخزين وقدرة حسابية كبيرة. كما أنهم مسؤولين عن الحفاظ على دفتري الأستاذ الموزع ، أثناء توفير الإدلة لمقاومة التحديات واستكمال المراجعة العامة .

ج. المنظم (R) مسؤول أيضًا عن الحفاظ على دفتري الأستاذ الموزع أثناء الإشراف على عملية المراجعة العامة وإدارة المراجعة العامة المتبادلة لتقنية سلاسل الثقة (PMAB) .

– بروتوكول المراجعة العامة المتبادلة لتقنية سلاسل الثقة (PMAB):

ينقسم إلى مرحلة الإعداد ومرحلة المراجعة. يتم تهيئة متغيرات النظام وإعداد المراجعة في مرحلة الإعداد. تشمل مرحلة المراجعة العملية التفصيلية لمراجعة البيانات والحصول على أدلة المراجعة والتحقق منها ، بالإضافة إلى تسوية الائتمان. بالإضافة إلى ذلك ، من أجل التحقق من البيانات عن بعد للتشغيل الديناميكي في الوقت المناسب ، يدعم PMAB المراجعة الديناميكية. حيث يدعم مالكى البيانات DO في مراجعة البيانات بعد العمليات الديناميكية ، والتي تتكون أساسًا من الإدراج والتعديل والحذف .لا تستطيع العقد المتآمرة خداع المنظم (R) بإرسال تحقق خاطئ لتجاوز كتل البيانات التالفة. والحافز على ذلك أن السلوك النزيه هو أكثر ربحية من التواطؤ. (Hanzhe Yang, June 2021) (Ning Lu, May 2020)

٢. أهداف المراجعة العامة المتبادلة لتقنية سلاسل الثقة (PMAB) :

- **مقاومة التطفل : يجب على المراجعة العامة المتبادلة لتقنية سلاسل الثقة (PMAB) منع الفاسدين من مقدمى الخدمات السحابية من التطفل على التحقق من المراجعة .**
- **الحفاظ على الخصوصية : يقتصر المشاركة في عقد المراجعة فقط على مقدمى الخدمات السحابية والمنظم ومالكى البيانات ، لكن لا يمكن لجميع الكيانات الأخرى الحصول على الهوية المحددة ومعلومات بيانات المصادر الخارجية لمالكى البيانات .**
- **مقاومة الغش: المراجعة تثبت الغش عن طريق أن الفاسد من مقدمى الخدمات السحابية لا يستطيع أن يجتاز التحقق من المراجعة .**
- **مقاومة الإحلال : بالنسبة لمقدم الخدمات السحابية الغير نزيه ، عند الحصول على أدلة المراجعة ، لا يمكنه استخدام مجموعة المعلومات المتعلقة بكتلة البيانات السليمة للحصول على دليل خاص بكتلة البيانات التالفة.**
- **الكفاءة: يجب أن يقتصر متوسط تكلفة دفعة المراجعة في بروتوكول المراجعة الخاص بالمراجعة العامة المتبادلة لتقنية سلاسل الثقة (PMAB) لمستوى منخفض جدًا وثابت ، ويجب التحكم في وقت التحقق الشامل للمراجعة العامة المتبادلة لتقنية سلاسل الثقة (PMAB) ليكون خلال فترة محددة .**

- **المراجعة الآلية: يجب أن تقوم المراجعة العامة المتبادلة لتقنية سلاسل الثقة (PMAB) بإجراء مراجعة تلقائية بشكل دوري على أساس عقود المراجعة .**
- **المراجعة الديناميكية: البيانات البعيدة التي يتم تعديلها ديناميكياً يمكن مراجعتها في الوقت المناسب وبشكل فعال .**

في المراجعة العامة المتبادلة لتقنية سلاسل الثقة (PMAB)، يتم إستخدام بشكل مبتكر المراجعة المتبادلة بين مقدمى الخدمات السحابية CSPs بدلاً من مراجعة(Third Party Auditor(TPA.حيث يتم تصميم آلية تحفيز تستند إلى الائتمان ، بحيث لا يكون أي من مقدمى الخدمات السحابية على استعداد لمساعدة غيرهم من مقدمى الخدمات السحابية الآخرين في إخفاء مشاكل البيانات. بالإضافة إلى الاعتماد على Ouroboros ، وبذلك فإن المراجعة العامة المتبادلة لتقنية سلاسل الثقة (PMAB) هو بروتوكول مراجعة يتكامل مع blockchain لإكمال عمليات المراجعة العامة بكفاءة وتلقائية . (Aggelos Kiayias, August 20–24, 2017)

٣. مفهوم الـ Ouroboros :

هو أول برتوكول من نوعه لتقنية سلاسل الثقة Blockchain لإثبات الحصة ولإثبات الأمان تم تطويره بواسطة Aggelos Kiayias و Alexander Russel و Bernardo David و Roman Oliynykov. يبدأ البروتوكول بـ "حصة ثابتة" حيث يتم تخصيص كتل blockchain للقادة بناءاً على حصتهم الأولية. بمجرد تخصيص الحصة الأولية للقادة ، يتم تخصيص حصة فعالة لكل قائد والتي تحدد بشكل نسبى توزيع البروتوكولات أثناء تنفيذها. (Ouroboros (blockchain), 2020) .

وهو نموذج يضفى صفة الرسمية على مشكلة فهم بروتوكول blockchain القائم على خوارزمية أثبات الصحة Proof of Stake (PoS) النموذج يركز على الثبات وتزامن العمليات ، وهما خاصيتان رسميتان لدفتر الأستاذ المعاملات الجيد. وهذا يجعل المعاملات التي تم إنشاؤها بصدق يتم تبنيها وتصبح غير قابلة للتغيير . (Aggelos Kiayias, August 20–24, 2017, p. 359)

٤. خوارزمية أثبات الصحة Proof of Stake (PoS) :

(الضحوي، ٢٠٢٠، صفحة ٤) (Ayushi sharma, 18 June 2021)

هي من أشهر خوارزميات الاتفاق أو الإجماع وهي عبارة عن خوارزميات تسمح للعُقد أو الأجهزة داخل تقنية سلاسل الثقة Blockchain بالوصول إلى إجماع حول الكتل التي تضاف إلى تقنية سلاسل الثقة Blockchain ، وهناك العديد من هذه الخوارزميات أشهرها:

- **خوارزمية إثبات العمل Proof-of-Work (PoW) : وهي من أشهر هذه الخوارزميات المستخدمة في البتكوين، حيث تعتمد على منح مكافأة مالية للتحقق من صحة المعاملات ، بعد التأكد من صحة بيانات المعاملة تعمل أجهزة الشبكة على تخمين رمز الكتلة من خلال حل معاملات حسابية، وعندما يتوصل أحد الأجهزة إلى الحل يتم إنشاء الكتلة داخل تقنية سلاسل الثقة Blockchain ويحصل المنقب على مكافأة مالية، لذلك تسمى بعملية التنقيب أو التعدين، تحتاج هذه العملية إلى قوة حوسبية كبيرة ومعالجات متخصص في حل المسائل الرياضية ليتمكن المنقب من إنشاء الكتلة والحصول على المكافأة .**

- **خوارزمية إثبات الحصة Proof-of-Stake (PoS) : تتطلب هذه الخوارزمية وجود مبلغ مالي في محافظ العاملين في الشبكة ولا يطلق عليهم هنا منقبون، إلا أنهم لا يقومون بعمليات التنقيب عن رمز للكتلة، ولكن بعد عملية التحقق من المعاملات والتأكيد عليها يتم رفع الكتلة إلى الشبكة ويحصل الجميع على مكافأة مالية، ولكن في حال تلاعب أحد الأجهزة بالبيانات فإن تقنية سلاسل الثقة Blockchain تسحب العملات الرقمية من محفظته كغرامة مالية، ولا تحتاج هذه الخوارزمية إلى قوة حوسبية أو معالجات ضخمة. وبذلك فإنها تحفز مقدمى الخدمات السحابية (CSPs) على النزاهة في المراجعة والبعد عن الغش والتواطؤ.**

٥. هيكل تقنية سلاسل الثقة Blockchain للمراجعة العامة المتبادلة لتقنية سلاسل الثقة (PMAB) :

(Hanzhe Yang, June 2021, p. 3)

هندسة Blockchain هي التصميم الأساسي لـ PMAB ، والذي يتكون بشكل أساسي من جزأين ، وهما سلسلة الائتمان (أي آلية الحوافز) وسلسلة المراجعة. آلية الحوافز هي مصدر الطاقة وحجر الزاوية الأمني في نظام blockchain. القيمة الائتمانية هو جوهر آلية حوافز PMAB ، والتي تأتي بشكل أساسي من الائتمان الأولي لمقدمى الخدمات السحابية ، والإيداع ، ومكافأة أجر المراجعة التي يدفعها مالكى البيانات DOs. العقدة المرشحة ذات الائتمان الأعلى تكون أكثر احتمالاً للاختيار كعقدة نموذجية. علاوة على ذلك ، فإن الائتمان المفقود بسبب التواطؤ(الاحتيال) سوف يفوق الائتمان المكتسب ، وسيقوم مقدمى الخدمات السحابية ذات الثقة بإجراء عمليات مراجعة نزيهه لتعظيم الفوائد.

عندما ينضم كل من مقدمى الخدمات السحابية إلى المراجعة العامة المتبادلة لتقنية سلاسل الثقة PMAB ، فإنه يحتاج إلى دفع بعض الودائع مقابل الائتمان الأولي ، والذي سيتم مصادرتها عند اكتشاف غش من قبل مقدم الخدمات السحابية.وتمثل قيمة البيانات هي قيمة التعويض المدفوعة من مقدم الخدمة السحابية إلى مالك البيانات عند فشل المراجعة ، ويتم وضع الائتمان الأولي والغرامات التي تم مصادرتها في مجمع المكافأت ، وسيقوم مقدمى الخدمات السحابية الذين يتمتعوا بالنزاهة والمشاركون في المراجعة بتقسيم المكافأة.

الكتلة وعقد المراجعة هي بنية البيانات الأساسية في سلسلة المراجعة. يخزن الكتلة (Block) محتويات ونتائج كل مراجعة. عقد المراجعة يحتفظ بالمعلومات المحددة لكل مهمة مراجعة. يتم تخزين العقد بالكامل في المنظم (R) ، ومالك البيانات المرتبط بالعملية DO ، ومقدم الخدمات السحابية CSP ، ويحتفظ جميع مقدمى الخدمات السحابية CSP بالرأس (Conheader) ، الذي يحدد معلومات مهمة المراجعة لكل مجموعة .

من خلال التحليل والعرض السابق يمكن بيان أهم نتائج البحث من خلال النقاط التالية :

١. تفتقر خدمات التخزين السحابية إلى الشفافية واللامركزية المحدودة كما أنها تواجه التحديات المتعلقة بالخصوصية والأمان.

٢. تقنية سلاسل الثقة blockchain تدعم وظيفة المراجعة وذلك من خلال تمكين التأكيد المستمر. حيث يستخدم blockchain كمستودع للبيانات بتحديث المعلومات (ومراجعتها) في الوقت الفعلي.

٣. لا يوجد مراجع طرف ثالث موثوق به تمامًا في العالم الحقيقي ، حيث قد يكشف عن بيانات المستخدم لتفعيل المنفعة الاقتصادية

٤. المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة تقوم بدور فعال فى مراجعة بيانات المصادر الخارجية للتخزين السحابى .

٥. المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة لمراجعة بيانات المصادر الخارجية للتخزين السحابى .تتم بكفاءة وتكلفة منخفضة ، كما أنها تحقق عوامل الأمان والشفافية والخصوصية .

وبناءاً على ذلك يتم رفض فرض العدم (لا يؤدى استخدام المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة إلى تفعيل مراجعة بيانات المصادر الخارجية للتخزين السحابى) وقبول الفرض البديل (يؤدى استخدام المراجعة العامة المتبادلة بإستخدام تقنية سلاسل الثقة إلى تفعيل مراجعة بيانات المصادر الخارجية للتخزين السحابى).

قائمة المراجع:

أولا –المراجع العربية:

أ. الدوريات العربية:

١. ايمن محمد صبري نخال. (٢٠٢٠). أثر استخدام تكنولوجيا سلسلة الكتل الرقمية (البلوك شين) على مسئولية مراجع الحسابات. الفكر المحاسبي ،جامعة عين شمس – كلية التجارة، مجلد ٢٤،عدد(١) ،صـ صـ ١–٥٨.

٢. حمادة السعيد المعصراوى غازى. (٢٠٢٠). محددات نجاح تبنى الشركات للأنظمة المحاسبية المعتمدة على تقنية سلسلة الكتل .Blockchain مجلة التجارة والتمويل ، جامعة طنطا – كلية التجارة،عدد خاص، صـ صـ ١–٣٠.

٣. سيد عبدالفتاح سيد. (٢٠١٩). أثر خصائص Blockchain على تحسين التقارير المالية الرقمية: دراسة ميدانية. مجلة الدراسات التجارية المعاصرة، العدد الثامن، صـ صـ ١٧٠–٢٠٥.

٤. مدى عبداللطيف الرحيلي ، هناء علي الضحوي. (٢٠٢٠). تطوير قطاع الإيجار العقاري بما يتماشى مع التحول الرقمي للمكلة العربية السعودية: دراسة مقترحة لتطبيق البلوك تشين Blockchain . مجلة دراسات المعلومات والتكنولوجيا، مجلد ٣ العدد ١، صـ صـ ١–٢٣.

٥. ممدوح على محمود. (٢٠١٥). استخدام التخزين السحابى للبيانات فى المكتبات ومراكز المعلومات وأمن المعلومات. المجلة الأردنية للمكتبات والمعلومات، مجلد ٥٠ عدد ٤، صـ صـ ١١–٤٨.

٦. ممدوح على محمود. (٢٠١٦). التخزين السحابي للبيانات وأمن المعلومات: دراسة تقييمية. المجلة الدولية لعلوم المكتبات والمعلومات، مجلد ٣(عدد ٤)، صـ صـ ١٩٦–٢١٨.

ثانياً : المراجع الإجنبية :

a. Periodicals:

1. Coyne, J. &. (2017). Can blockchains serve an accounting purpose? Journal of Emerging Technologies in Accounting, 14(2), P P 101-111.

2. Erica Pimentel,Emilio Boulianne,Shayan Eskandari,Jeremy Clark. (October 2020). Systemizing the Challenges of Auditing Blockchain-Based Assets. Journal of Information Systems, Vol 35(2), PP 1-43. Retrieved from https://www.researchgate.net/publication.

3. Hanzhe Yang ,Ruidan Su ,Pei Huang,Yuhan Bai,Kai Fan ,Kan Yang,Hui Li and Yintang Yang. (June 2021). PMAB: A Public Mutual Audit Blockchain for Outsourced Data in Cloud Storage. Security and Communication Networks, Volume 2021, Article ID 9993855, PP 1-11.

4. Hongtao Li , Feng Guo , Lili Wang, Jie Wang,Bo Wang and Chuankun Wu2. (2021). A Blockchain-Based Public Auditing Protocol with Self-Certified Public Keys for Cloud Data. Security and Communication Networks, Vol 2021, Article ID 6623639, PP 1-10. Retrieved from https://doi.org/10.1155/2021/6623639

5. M Husni, H T Ciptaningtyas, W Suadi, R M Ijtihadie, R Anggoro, M F Salam and and S Arifiani. (2020). Security audit in cloud-based server by using encrypted data AES -256 and SHA-256. Materials Science and Engineering, Vol 830(Issue 3), PP 1-6.

6. Najoua Elommal, Riadh Manita. (2021). HOW BLOCKCHAIN INNOVATION COULD AFFECT THE AUDIT. Journal of Innovation Economics & Management, 2021/O, PP 1-28. Retrieved from https://www.cairn.info/revue-journal-of-innovation-economics-2021-0-page-l103.htm

7. Ning Lu, Yongxin Zhang ,Wenbo Shi ,Saru Kumari ,Kim-Kwang Raymond Chood. (May 2020). A secure and scalable data integrity auditing scheme based on hyperledger fabric. Computers & Security, Vol 92, PP 1-16.

8. Song Li, Jian Liu,Guannan Yang and Jinguang Han. (2020). A Blockchain-Based Public Auditing Scheme for Cloud Storage Environment without Trusted Auditors. Wireless Communications and Mobile Computing,Volume 2020, Article ID 8841711, PP 1-13. Retrieved from https://doi.org/10.1155/2020/8841711

9. X. Jia, D. He, Q. Liu, and K.-K. R. Choo. (2018). An efficient provably-secure certificateless signature scheme for internet of things deployment. Ad Hoc Networks, Vol 71, PP 78–87.

b. Conferences :

1. Aggelos Kiayias, Alexander Russell,Bernardo David and Roman Oliynykov. (August 20–24,2017). Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. Advances in Cryptology – CRYPTO 2017,37th Annual International Cryptology Conference. Proceedings, Part I, pp. 357-388. Santa Barbara, CA, USA: Springer Nature.

2. Chunhua Li, Jiaqi Hu, Ke Zhou, Yuanzhang Wang,and Hongyu Deng. (September 2018). Using Blockchain for Data Auditing in Cloud. 4th International Conference, ICCCS 2018 ,pp 335-345. Haikou, China: ResearchGate. Retrieved from https://www.researchgate.net/publication.

3. Danilo Francati,Giuseppe Ateniese, Abdoulaye Fayey, Andrea Maria Milazzo,Angelo Massimo Perillo, Luca Schiattiy and Giuseppe Giordano. (May 2021). Audita: A Blockchain-based Auditing

Framework for Off-chain Storage. ACM Asia Conference on Computer and Communications Security, pp. 1-15. Retrieved from https://eprint.iacr.org/2019/1345.pdf

c. Web sites :

1. Ayushi sharma, S. T. (18 June 2021). Introduction to Blockchain. Retrieved from ResearchGate: https://www.researchgate.net/publication/352379328_Introduction_to_Blockchain

2. Dylan Yaga , Peter Mell ,Nik Roby ,Karen Scarfone. (2018). Blockchain Technology Overview. NISTIR 8202 . (Department of Commerce. National Institute of Standards and Technology. United State of America) Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf

3. Manikandan, Jayanthi. (Dec 30, 2019). Cloud computing roles and responsibilities. Retrieved from Infosectrain: https://www.infosectrain.com/blog/cloud-computing-roles-and-responsibilities/

4. Nath, Nishant. (Feb 17,2021). Role of Cloud Service Providers in Enterprise Data Management. Retrieved from go4hosting: https://go4hosting.com/blog/cloud-hosting/role-of-cloud-service-providers-in-enterprise-data-management/

5. Ouroboros (blockchain) . (2020) . Retrieved from Golden :https://golden.com/wiki/Ouroboros_(blockchain)-639P6WZ